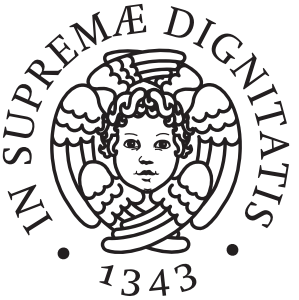
Università di Pisa



Faculty of Mathematics

Unique Factorization in the Ring of Integers of the Complex Quadratic Fields

Bachelor Degree Thesis
in Mathematics

Candidate
Lorenzo Furio

Supervisor
Davide Lombardo
Università di Pisa

Academic Year 2018 - 2019

Contents

Introduction

A question that arises spontaneously when one approaches the study of number fields and the relative rings of integers is whether or not they are rings with unique factorization. In general, fixed a field, it is always possible to calculate its ideal class group, but it is a very complex problem to determine which fields, within a set described by a fixed property, have a class number 1. However, if we consider particular families of number fields it is sometimes possible to exploit their characteristics to study the solution to this problem. In our case we will study imaginary quadratic fields in order to determine for which of them the relative ring of integers has unique factorization. One can easily see that the quadratic extensions of $\mathbb{Q}$ are all and only those of the form $\mathbb{Q}(\sqrt{m})$ for $m \in \mathbb{Z}$ squarefree. Therefore the complex quadratic fields, the only ones we will study, are $\mathbb{Q}(\sqrt{-m})$ for $m \in \mathbb{N}$ squarefree.
In 1801, in *Disquisitiones Arithmeticae* [Gau86], Gauss conjectured that if $K = \mathbb{Q}(\sqrt{-m})$, then $\mathcal{O}_K$ is a UFD if and only if $m \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Actually, the original Gauss conjecture was stated as a quadratic form problem, which turns out to be equivalent to the one stated above. The conjecture was proved later by Heegner [Hee52], Baker [Bak67] and Stark [Sta67]. Heegner's proof had been riformulated by Serre [Ser89] using elliptic curves and this is the proof that will be presented in this thesis. Note that we restricted to the complex quadratic fields because if $K = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{N}$ squarefree, it is conjectured that the rings of integers with unique factorization are infinite, but this fact still seems far from being proved.
In order to prove Gauss's conjecture we will start by noting that $\mathcal{O}_K$ is a lattice in $\mathbb{C}$, so $\mathbb{C}/\mathcal{O}_K$ is biolomorphic to an elliptic curve E. We can therefore study the properties of this curve to deduce the properties of $\mathcal{O}_K$. It can be shown that E is a CM curve and that its endomorphism ring is $\mathcal{O}_K$. Furthermore, assuming that $\mathcal{O}_K$ is a UFD, we will first show that its j-invariant is rational and then later obtain that it is integer. Then, we will observe how $\mathbb{C}$'s automorphisms act on the torsion points of the curve, determining some strict condition on j, which will allow us to show that there exists only a finite number of CM curves with integer j-invariant. This concludes the proof of the conjecture, noting that every $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ which is a UFD corresponds to a different elliptic curve with these properties. Furthermore, this method leads

to explicitly obtain these curves, making it possible to check the class numbers of all the $\mathbb{Q}(\sqrt{-d})$ fields found.
Let us now give a more precise description of the content of the thesis. In the first chapter we will introduce some basic results in the theory of elliptic curves that we will use in the next chapters. In the second chapter we will show that, given a complex quadratic field K, there exists a finite number of elliptic curves E up to isomorphism such that $\mathrm{End}(E) \cong \mathcal{O}_K$; to reach this result we will study how the group $\mathrm{Aut}(\mathbb{C})$ acts on the set of these curves. In the third chapter we will describe the theory of the Tate curve, that is an elliptic curve defined on a p-adic field whose points can be identified with a quotient $\bar{K}^*/q^{\mathbb{Z}}$. This has the property that the elements of $\mathrm{Gal}(\bar{K}/K)$ commute with the isomorphism between $\bar{K}^*/q^{\mathbb{Z}}$ and the group of the points of the curve. In fact, since elliptic curves with rational j-invariant can be defined over $\mathbb{Q}$, the curves $\mathbb{C}/\mathcal{O}_K$ of the previous chapter can be studied over an extenion of $\mathbb{Q}$ that doesn't lie in $\mathbb{C}$, in particular we will consider some p-adic fields.We will therefore end up deducing that if the j-invariant of an elliptic curve has negative p-adic evaluation for some prime p, its endomorphism ring is isomorphic to $\mathbb{Z}$, therefore the j-invariant of the CM curves has absolute value not greater than 1 for all primes, then it's an algebraic integer. From this it follows that if $\mathcal{O}_K$ is a UFD, the j-invariant of the curve $\mathbb{C}/\mathcal{O}_K$ is an integer. Finally in the fourth chapter we will study how the absolute Galois group of $\mathbb{Q}$ acts of the torsion points $E[\ell]$ for a prime ℓ, representing the automorphisms in $GL_2(\mathbb{F}_\ell)$. Using the theory of modular curves we will obtain a diophantine equation with finitely many solutions, i.e. there are finitely many elliptic curves up to isomorphism over $\mathbb{C}$ such that j satisfies the equation, in particular there are finitely many elliptic curves whose endomorphism ring is isomorphic to $\mathcal{O}_K$ and is a UFD. In addition, knowing the value of j allows to compute the effective curves and verify that the rings $\mathcal{O}_K$ with unique factorization are only the 9 found by Gauss.

CHAPTER 1

Preliminaries

In this section we will introduce some basic results that we will use in the next chapters.

1.1 The ideal class group

We begin observing some properties of $\mathcal{O}_K$:

Proposition 1.1.1. *Let K be a number field and $\mathcal{O}_K$ its ring of integers, then $\mathcal{O}_K$ is a UFD if and only if it's a PID.*

We then define a particular group, named the ideal class group, in the following way:

Definition 1.1.2. Named $\mathcal{F}(K)$ the fractional ideals of $\mathcal{O}_K$ and $\mathcal{P}(K)$ the principal ideals among the fractional ideals, we define $Cl(K) := \frac{\mathcal{F}(K)}{\mathcal{P}(K)}$ to be the ideal class group of $\mathcal{O}_K$.

In fact, $\mathcal{F}(K)$ is an abelian group whose opration is the multiplication and $\mathcal{P}(K)$ is a subgroup, then the quotient is well defined. The ideal class group has the following property:

Theorem 1.1.3. *Let K be a number field, then $Cl(K)$ is a finite group.*

The ideal class group "measure" how much a ring of integers fails to be a PID, in particular it is not difficult to note that $\mathcal{O}_K$ is a PID (and then a UFD) if and only if $Cl(K)$ is trivial.

1.2 Elliptic curves

The following results aim to report the basic properties of the endomorphisms of an elliptic curve and to show the connection with the rings of the integers of the complex quadratic fields.
When we consider elliptic curves over complex numbers, there is a corrispondence between elliptic curves and complex tori, i.e. the quotients of $\mathbb{C}$ by a lattice Λ, a discrete subgroup of rank 2. From now on we will call *torus* a quotient $\mathbb{C}/\Lambda$.

Definition 1.2.1. Let T_1, T_2 be tori, we call an isogeny an additive surjective holomorphic homomorphism $c : T_1 \to T_2$.

Proposition 1.2.2. *For every isogeny $c : T_1 \to T_2$ there exists a constant $\alpha \in \mathbb{C}^*$ such that $c([x]) = [\alpha \cdot x] \quad \forall x \in \mathbb{C}$.*

Definition 1.2.3. Let T be a torus, we define the set of the endomorphisms of the torus to be $\mathrm{End}(T) := \{c : T \to T | c \text{ è un'isogenia}\} \bigcup \{0\}$.

In the previous definition the isogenies are meant to be elements of $\mathbb{C}^*$, rather than functions.

Proposition 1.2.4. $\mathrm{End}(T)$ *is a subring of $\mathbb{C}$ whose elements are algebraic integers with degree at most 2.*

We can note that $\mathbb{Z} \subset \mathrm{End}(T)$, in addition $\mathrm{End}(T)$ is a discrete subgroup of $\mathbb{C}$, then it's a free $\mathbb{Z}$-module generated by 1 or 2 elements. In particular $\mathrm{End}(T) = \mathbb{Z}$ or $\mathrm{End}(T) = \mathbb{Z}[\alpha]$, where α is an algebraic integer of degree 2.
A torus is a complex variety of dimension 1, then we want to find a curve in $\mathbb{P}^2\mathbb{C}$ which is biolomrphic to the torus, in particular we want to find a correspondece between curves and tori.

Definition 1.2.5. Let K be a field, we define an elliptic curve to be a non-singular plane algebraic curve defined over K by an equation in $\mathbb{P}^2K$ of the form

$$E : \; Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

In this thesis we will mainly deal with complex curves.

Definition 1.2.6. We define the Weierstrass function to be

$$\wp := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(\omega - z)^2} - \frac{1}{\omega^2} \right)$$

The Weierstrass function is diperiodic respect to the lattice Λ, therefore we can consider it as a function $\wp : {}^{\mathbb{C}}\!/_{\Lambda} \to \mathbb{C}$. Furthermore, it's not difficult to show that such a function is meromorphic and has poles of order 2 in the elements of the lattice; equivalently we can consider it as a holomorphic function $\wp : {}^{\mathbb{C}}\!/_{\Lambda} \to \mathbb{P}^2\mathbb{C}$.

Proposition 1.2.7. *The functions $\wp(z)$ and $\wp'(z)$ satisfy an equation of the form*

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

where

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$$
$$g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

Proposition 1.2.8. *The following function*

$$\begin{aligned} z &\longmapsto [\wp(z), \wp'(z), 1] \quad \text{if } z \neq 0 \\ z &\longmapsto [0,1,0] = O \quad \text{if } z = 0 \end{aligned}$$

is a biolomorphism between $T = {}^{\mathbb{C}}\!/_{\Lambda}$ and the curve $E : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ in $\mathbb{P}^2\mathbb{C}$.

Proposition 1.2.9. *Let Λ be a lattice, every meromorphic Λ-periodic function is a rational function of $\wp$ and $\wp'$.*

In general we will represent the curve with its equation over $\mathbb{C}^2$, adding a point at infinity corresponding to O.
We will refer to the curve obtained by a torus of lattice Λ as E_Λ.
Starting from the group law of T it is possible to define a group law on the curve such that the biolomorphism in the proposition 1.2.8 is a homomorphism. Intuitively, we define the sum of the points P and Q as the third point of intersection between the curve and the line PQ whose coordinate y has opposite sign. For $x_1 \neq x_2$, this corresponds to the following algebraic relation (on affine coordinates):

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{k^2}{4} - x_1 - x_2 \ , \ -k\left(\frac{k^2}{4} - x_1 - x_2 \right) - h \right) \tag{1.1}$$

where $k = \frac{y_2 - y_1}{x_2 - x_1}$ and $h = y_1 - kx_1$. If $x_1 = x_2$ then we have two cases: either $y_1 = -y_2 \neq -y_1$, then we set $(x_1, y_1) + (x_2, y_2) = O$, with O being the point at infinity; or $(x_1, y_1) = (x_2, y_2)$, then the same relation of 1.1 holds, but $k = \frac{12x_1^2 - g_2}{2y_1}$ and $h = y_1 - kx_1$.
For elliptic curves which are not in the form $y^2 = 4x^3 - g_2x - g_3$ we know that there exist a linear change of coordinates that sends it in such a form, therefore

the group law on a generic curve is defined to be the one of the correspondent curve in the form $y^2 = 4x^3 - g_2x - g_3$, with a change of coordinates.
It is not difficult to note that the group law described in the equation 1.1 is a function whose coordinates are rational functions of the point of the curve, with rational coefficients. Furthermore, the coordinates change that sends an elliptic curves of the form $y^2 = 4x^3 - g_2x - g_3$ in one in the Weierstrass form, i.e. in the form $y^2 = x^3 + ax + b$, has rational coefficients, then the group law on elliptic curves in Weierstrass form has coordinates which are rational functions with rational coefficients.

Definition 1.2.10. The group

$$E[n] := \{P \in E | nP = 0\}$$

is called the n-torsion group.

Proposition 1.2.11. $E[n] \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$

We will say that two elliptic curves are isomorphic if there exist a holomorphic isomorphism between them, i.e. a function between the curves whose coordinates are holomorphic functions and that is an isomorphism respect to the group laws of the curves. In general we can consider holomorphic homomorphisms, in particular we can definethe ring of the endomorphisms of the curve $\mathrm{End}(E)$. Given an elliptic curve E_Λ obtained by a lattice Λ, the ring of the endomorphisms of the curve is isomorphic to the ring of the endomorphisms of the torus ${}^{\mathbb{C}}\!/_{\Lambda}$, because there exists a holomorphic isomorphism between the curve and the torus.
If we are handling elliptic curves over fields different from $\mathbb{C}$ we cannot use the holomorphy condition to define the endomorphisms anymore, then we can use the following:

Definition 1.2.12. Let K be a field and ${}^{E}\!/_{K}$ an elliptic curve defined over it, we call endomorphism of the curve an algebraic function $E \longrightarrow E$ that induces a group homomorphism.

Proposition 1.2.13. $E_{\Lambda_1} \cong E_{\Lambda_2} \iff \exists \alpha \in \mathbb{C}$ *such that* $\Lambda_1 = \alpha\Lambda_2$.

We note that a linear coordinate change is an isomorphism of elliptic curves. In addition, given a generic curve of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, defined over a field of characteristic different from 2 and 3, there always exists a linear coordinates transformation that sends it in an elliptic curve in Weierstrass form, i.e. in the form $y^2 = x^3 + ax + b$. Therefore we can always assume that an elliptic curve is in Weierstrass form, up to isomorphism.

Definition 1.2.14. Given a generic elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

define:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2^2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6
\end{aligned}$$

In addition we define the j-invariant of the curve to be $j = \frac{c_4^3}{\Delta}$.

Theorem 1.2.15. *The j-invariant of a curve is invariant under isomorphism.*

This theorem allows us to define the j-invariant just for curves in the Weierstrass form without loss of generality, then for the curve $y^2 = x^3 + ax + b$ we have $\Delta = 4a^3 + 27b^2$ and $j = \frac{1728a^3}{\Delta}$.
The curve $y^2 = 4x^3 - g_2x - g_3$ has $j = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$.

Theorem 1.2.16. *Two elliptic curves defined over an algebraically closed field are isomorphic if and only if have the same j-invariant.*

Theorem 1.2.17. $\forall c \in \mathbb{C}\ \exists \Lambda$ *lattice such that* $j(E_\Lambda) = c$.

Corollary 1.2.18. *Every complex elliptic curve, up to isomorphism, comes from a torus.*

Proposition 1.2.19. *For complex elliptic curves the definition of endomorphism like in 1.2.12 is the same of the definition of holomorphic endomorphism inherited from the tori.*

Proof. The rational functions are clearly holomorphic in the projective plane, then we just need to prove that the holomorphic homomorphisms consists of rational functions.
We know that $E \cong E_\Lambda$ for some lattice Λ, then $\forall \phi$ holomorphic homomorphism of E $\exists \alpha \in \text{End}\left(\mathbb{C}/\Lambda\right)$ such that $\phi(\wp(z), \wp'(z)) = (\wp(\alpha z), \wp'(\alpha z))$. Since $\alpha\Lambda \subseteq \Lambda$, the function $\wp(\alpha z)$ is Λ-periodic, therefore, for the proposition 1.2.9, it is a rational function of $\wp(z)$ and $\wp'(z)$. □

Example 1.2.20. Given the curve $E:\ y^2 = x^3 + x$, the function $(x, y) \longmapsto (-x, iy)$ is and endomorphism and its coordinates are rational functions.

So fare, we mainly dealt with complex elliptic curves because we can establish a correspondence between such curves and complex tori. In general, for elliptic curves defined over a generic field, not all the properties listed above remain valid, but some of them do not depend on the particular choice of the field, for example the theorem 1.2.16. In chapter 3, we will define also some elliptic curves over number fields or their completions respect to some non archimedean places.
Given these introductive properties, in order to study the ring $\mathcal{O}_K$ of integers of $K = \mathbb{Q}(\sqrt{-n})$, we will start considering the elliptic curves whose endomorphism ring is isomorphic to a $\mathcal{O}_K$.

CHAPTER 2

Rationality of the j-invariant

2.1 The action of $Cl(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$

Definition 2.1.1. Let R be a ring, we define the following set:

$$\mathcal{ELL}(R) := \{E|\,\mathrm{End}(E) \cong R\}_{/\cong} \longleftrightarrow \{\Lambda|\,\mathrm{End}(E_\Lambda) \cong R\}_{/\text{omotetia}}$$

where E is a complex elliptic curve andΛ is a lattice in $\mathbb{C}$.

Lemma 2.1.2. *Let $n \in \mathbb{N} \setminus \{0\}$ and $K = \mathbb{Q}(\sqrt{-n})$, then $\mathcal{ELL}(\mathcal{O}_K) \neq \emptyset$.*

Proof. Let's consider the lattice $\Lambda = \mathcal{O}_K$ and the curve $E = {}^{\mathbb{C}}\!/_{\mathcal{O}_K}$, therefore $\mathcal{O}_K \cdot \mathcal{O}_K \subset \mathcal{O}_K$, then $\mathcal{O}_K \subset \mathrm{End}(E)$. Furthermore, if $\alpha \in \mathrm{End}(E)$, $\alpha\mathcal{O}_K \subset \mathcal{O}_K$, then $\alpha \in K$. We know that a curve's endomorphism is always an algebraic integer, thus $\alpha \in \mathcal{O}_K$, hence $\mathrm{End}(E) = \mathcal{O}_K$. In particular, this implies that $E \in \mathcal{ELL}(\mathcal{O}_K)$, meaning that E stands for its isomorphism class. □

From now on, given an elliptic curve, we will write that the curve belongs to $\mathcal{ELL}(R)$ to mean that its isomorphism class belongs to that set.
We will also use this notation: let A and B be $\mathbb{Z}$-submodules of $\mathbb{C}$, we will write AB to indicate the module $< \{ab \mid a \in A, b \in B\} >_{\mathbb{Z}}$, similar to the notation used for the fractional ideals.
At last, from now on we fix K to be a complex quadratic field, unless otherwise specified.
Let's now consider a fractional ideal $\mathfrak{a} \in \mathcal{F}(K)$. This is always a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, hence, in the case in which $K = \mathbb{Q}(\sqrt{-n})$, $\mathfrak{a} \subset \mathbb{C}$ is a $\mathbb{Z}$-module of rank 2; in addition $\mathfrak{a} \subsetneq \mathbb{R}$, then $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Therefore we can consider the elliptic curve $E_\mathfrak{a}$ and note that

$$\begin{aligned}\mathrm{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \{\alpha \in K \mid (\alpha)\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1}\} = \\ = \{\alpha \in K \mid (\alpha) \subseteq \mathcal{O}_K\} = \mathcal{O}_K\end{aligned}$$

Hence $E_{\mathfrak{a}} \in \mathcal{ELL}(\mathcal{O}_K)$. This remark leads to the following proposition.

Proposition 2.1.3. *Let Λ be a lattice such that $\mathrm{End}(E_\Lambda) \cong \mathcal{O}_K$, then $\exists \lambda \in \mathbb{C}$ and $\exists \mathfrak{a} \in \mathcal{F}(K)$ such that $\Lambda = \lambda\mathfrak{a}$.*

Proof. We know that every lattice can be normalized, i.e. $\exists \lambda \in \Lambda$ such that $\frac{1}{\lambda}\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$. By hypothesis $\mathcal{O}_K\Lambda = \Lambda$, then

$$\mathcal{O}_K \frac{1}{\lambda}\Lambda = \frac{1}{\lambda}\Lambda \implies \mathcal{O}_K(\mathbb{Z} \oplus \tau\mathbb{Z}) = \mathbb{Z} \oplus \tau\mathbb{Z}$$

However $\mathcal{O}_K\mathbb{Z} = \mathcal{O}_K$, hence

$$\mathcal{O}_K \subseteq \mathcal{O}_K \oplus \tau\mathcal{O}_K\mathbb{Z} = \mathbb{Z} \oplus \tau\mathbb{Z}$$

Moreover $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$, but $\mathcal{O}_K \subseteq \mathbb{Z} \oplus \tau\mathbb{Z} \subseteq \mathbb{Q}(\tau)$, then $K \subseteq \mathbb{Q}(\tau)$. Since $[\mathbb{Q}(\tau) : \mathbb{Q}] = [K : 2]$ we get that $\mathbb{Q}(\tau) = K$. We conclude that $\frac{1}{\lambda}\Lambda$ is a $\mathcal{O}_K$-submodule of K, then it is a fractional ideal, that is $\frac{1}{\lambda}\Lambda = \mathfrak{a} \in \mathcal{F}(K) \implies \Lambda = \lambda\mathfrak{a}$. □

Proposition 2.1.4. *Let $\mathfrak{a} \in \mathcal{F}(K)$ and let Λ be a lattice in $\mathbb{C}$ such that $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, then $\mathfrak{a}\Lambda$ is a lattice and $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$.*

Proof. For a fixed $\mathfrak{b} \in \mathcal{F}(K)$ we know that $\mathfrak{a}\Lambda = \mathfrak{a}\lambda\frac{1}{\lambda}\Lambda = \lambda\mathfrak{a}\mathfrak{b}$ that is a lattice in $\mathbb{C}$, furthermore

$$\begin{aligned}\mathrm{End}(E_{\mathfrak{a}\Lambda}) &= \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}\} = \\ &= \{\alpha \in K \mid (\alpha) \subseteq \mathcal{O}_K\} = \mathcal{O}_K\end{aligned}$$

then $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$. □

Proposition 2.1.5. *Let $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(K)$ and let Λ be a lattice in $\mathbb{C}$, then*

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \text{ in } Cl(K)$$

Proof.

$$\begin{aligned}&E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \\ &\exists \alpha \in \mathbb{C} \text{ tale che } \alpha\mathfrak{a}\Lambda = \mathfrak{b}\Lambda \iff \\ &\exists \alpha \in \mathbb{C} \text{ tale che } \alpha\Lambda = \mathfrak{a}^{-1}\mathfrak{b}\Lambda \iff \\ &\exists \alpha \in \mathbb{C} \text{ tale che } \alpha\frac{1}{\lambda}\Lambda = \mathfrak{a}^{-1}\mathfrak{b}\frac{1}{\lambda}\Lambda \iff \\ &\exists \alpha \in K \text{ tale che } \alpha = \mathfrak{a}^{-1}\mathfrak{b} \iff \\ &\mathfrak{a}^{-1}\mathfrak{b} \in \mathcal{P}(K) \iff \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \text{ in } Cl(K)\end{aligned}$$

□

The last three propositions allow us to define an action of the ideal class group on the set $\mathcal{ELL}(\mathcal{O}_K)$. The following theorem aims to describe this action.

Theorem 2.1.6. *The group $Cl(K)$ acts on $\mathcal{ELL}(\mathcal{O}_K)$ as*

$$\begin{array}{ccc} Cl(K) \times \mathcal{ELL}(\mathcal{O}_K) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \bar{\mathfrak{a}} * E_\Lambda & \longmapsto & E_{\mathfrak{a}\Lambda} \end{array}$$

Moreover, this action is simply transitive.

Proof. We first note that this action is well defined, i.e. $E_{\mathfrak{a}\Lambda}$ doesn't depends on the choice of the element of the class of $\mathfrak{a}$, indeed for the proposition 2.1.5 if two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ belongs to the same class then $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$. We now show that the action is simply transitive, i.e. for every two elements in $\mathcal{ELL}(\mathcal{O}_K)$ there exists a unique class in $Cl(K)$ that sends an element in the other. Let then Λ_1, Λ_2 be two latticessuchhe that $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{ELL}(\mathcal{O}_K)$, we know that for the proposition 2.1.3, $\Lambda_1 = \lambda_1\mathfrak{a}$ and $\Lambda_2 = \lambda_2\mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(K)$. Hence

$$\begin{aligned} &\exists \mathfrak{c} \in \mathcal{F}(K) \text{ tale che } E_{\mathfrak{c}\Lambda_1} \cong E_{\Lambda_2} \iff \\ &\exists \alpha \in \mathbb{C} \text{ tale che } \alpha\mathfrak{c}\Lambda_1 = \Lambda_2 \iff \\ &\frac{\alpha\lambda_1}{\lambda_2}\mathfrak{c}\mathfrak{a} = \mathfrak{b} \iff \\ &\overline{\mathfrak{c}\mathfrak{a}} = \overline{\mathfrak{b}} \text{ in } Cl(K) \iff \bar{\mathfrak{c}} = \overline{\mathfrak{a}^{-1}\mathfrak{b}} \end{aligned}$$

Therefore the action is transitive, because $\overline{\mathfrak{a}^{-1}\mathfrak{b}} * E_{\Lambda_1} = E_{\Lambda_2}$. Finally we note that for the proposition 2.1.5, if the fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ maps the curve E_Λ to the same element, then $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \implies \bar{\mathfrak{a}} = \bar{\mathfrak{b}}$. □

Corollary 2.1.7. *$|\mathcal{ELL}(\mathcal{O}_K)| = |Cl(K)|$, in particular $\mathcal{ELL}(\mathcal{O}_K)$ is a finite set.*

2.2 Algebraicity of the j-invariant

We are now interested in studying the behaviour of the ring operations of $\mathrm{End}(E)$. If the complex elliptic curve E is related to a torus T, then $\mathrm{End}(T)$ is a subring of $\mathbb{C}$ and inherits its operations, hence, in order to better understand the behaviour of the operations of $\mathrm{End}(E)$ we need to push forward the operations of $\mathrm{End}(T)$ with the function $z \longmapsto (\wp(z), \wp'(z))$. Hence, if $\alpha, \beta \in \mathrm{End}(T)$, in $\mathrm{End}(E)$ they become

$$\phi = \{(\wp(z), \wp'(z)) \mapsto (\wp(\alpha z), \wp'(\alpha z))\}\ ,\ \psi = \{(\wp(z), \wp'(z)) \mapsto (\wp(\beta z), \wp'(\beta z))\}$$

Then

$$\begin{aligned}\phi \cdot \psi &= \{(\wp(z), \wp'(z)) \mapsto (\wp(\alpha\beta z), \wp'(\alpha\beta z))\} = \\ &= \phi(\{(\wp(z), \wp'(z)) \mapsto (\wp(\beta z), \wp'(\beta z))\}) = \phi \circ \psi\end{aligned}$$

thus we note that the product in the ring $\mathrm{End}(E)$ is the composition of functions. To explicit the sum, if $(x, y) = (\wp(z), \wp'(z))$, we have

$$\begin{aligned}(\phi + \psi)(x, y) &= (\wp((\alpha + \beta)z), \wp'((\alpha + \beta)z)) = \\ &= (\wp(\alpha z + \beta z), \wp'(\alpha z + \beta z)) = \\ &= (\wp(\alpha z), \wp'(\alpha z)) + (\wp(\beta z), \wp'(\beta z)) = \phi(x, y) + \psi(x, y)\end{aligned}$$

Where the sum of the point of the curve is the group law described in the equation 1.1, in particular, its coordinates are rational functions of the coordinates of $\phi(x, y)$ and $\psi(x, y)$.

Remark 2.2.1. $\mathrm{End}(E) \cong \mathrm{End}(T)$ is a commutative ring, hence the composition of two endomorphism of an elliptic curve is a commutative operation.

We now begin to study how the automorphisms of $\mathbb{C}$ are interacts with the complex elliptic curves. In particular, given the curve $E : \ y^2 = x^3 + ax + b$, we set σE to be the curve obtained applying the automorphism $\sigma \in \mathrm{Aut}(\mathbb{C})$ to its equation, that is, σE is the elliptic curve defined by the equation $\sigma E : y^2 = x^3 + \sigma(a)x + \sigma(b)$.

Proposition 2.2.2. *Let $\sigma \in \mathrm{Aut}(\mathbb{C})$, let E be a complex elliptic curve, then $\mathrm{End}(\sigma E) \cong \mathrm{End}(E)$.*

Proof. We first show that $\mathrm{End}(\sigma E) = \sigma\,\mathrm{End}(E)$, where σ acts on the endomorphisms by acting on their coefficients. If $E : \ y^2 = x^3 + ax + b$, then $\sigma E : \ y^2 = x^3 + \sigma(a)x + \sigma(b)$ and the points $(x, y) \in E$ are sent in the points $(\sigma(x), \sigma(y)) \in \sigma E$. Since every $\phi \in \mathrm{End}(\sigma E)$ is a rational function, it can be written in the form

$$\phi(u, v) = \left(\frac{p_1(u, v)}{q_1(u, v)}, \frac{p_2(u, v)}{q_2(u, v)}\right) \quad \text{dove} \quad p_1, p_2, q_1, q_2 \in \mathbb{C}[u, v]$$

the we obtain

$$\phi\left(\sigma(x), \sigma(y)\right) = \left(\frac{p_1(\sigma(x), \sigma(y))}{q_1(\sigma(x), \sigma(y))}, \frac{p_2(\sigma(x), \sigma(y))}{q_2(\sigma(x), \sigma(y))}\right)$$

however, for every polynomial $f(x, y) = \sum_{i,j} c_{i,j} x^i y^j \in \mathbb{C}[x, y]$ we have

$$f(\sigma x, \sigma y) = \sum_{i,j} c_{i,j} \sigma(x)^i \sigma(y)^j = \sum_{i,j} \sigma(\sigma^{-1}(c_{i,j}) x^i y^j) = \sigma((\sigma^{-1} f)(x, y))$$

Therefore $\phi(\sigma(x),\sigma(y)) = \sigma((\sigma^{-1}\phi)(x,y))$, hence $(\sigma^{-1}\phi)(x,y) \in E$. It follows that $\sigma^{-1}\phi(E) \subset E$, then, in order to show that $\sigma^{-1}\phi \in \mathrm{End}(E)$, we just need to prove that it is a homomorphism. Lets consider the following equalities:

$$\begin{aligned}(\sigma^{-1}\phi)((x,y)+(x',y')) &= \sigma^{-1}(\phi(\sigma((x,y)+\sigma(x',y')))) = \\ &= \sigma^{-1}(\phi((\sigma(x),\sigma(y))+(\sigma(x'),\sigma(y')))) = \\ &= \sigma^{-1}(\phi(\sigma(x),\sigma(y))+\phi(\sigma(x'),\sigma(y'))) \overset{*}{=} \\ &\overset{*}{=} \sigma^{-1}(\phi(\sigma(x),\sigma(y)))+\sigma^{-1}(\phi(\sigma(x'),\sigma(y'))) = \\ &= (\sigma^{-1}\phi)(x,y)+(\sigma^{-1}\phi)(x',y')\end{aligned}$$

where the equality (*) holds because the group law of the curve is a rational function with rational coefficients, then commutates with σ. We have proved that $\mathrm{End}(\sigma E) \subseteq \sigma\,\mathrm{End}(E)$, however, with the same reasoning in the opposite direction, it is easy to see that the other inclusion is also valid, obtaining the desired equality.
Now we just need to prove that $\mathrm{End}(E) \cong \sigma\,\mathrm{End}(E)$. To do that, it is sufficient to show that σ is a ring homomorphism for $\mathrm{End}(E)$ and it is injective. If $\phi,\psi \in \mathrm{End}(E)$ then $\forall (x,y) \in E$

$$\begin{aligned}\sigma(\phi\circ\psi)(x,y) &= \sigma(\phi(\psi(\sigma^{-1}(x),\sigma^{-1}(y)))) = \\ &= \sigma\phi(\sigma(\psi(\sigma^{-1}(x),\sigma^{-1}(y)))) = \\ &= \sigma\phi(\sigma\psi(x,y))\end{aligned}$$

That is $\sigma(\phi\circ\psi) = \sigma\phi\circ\sigma\psi$. Furthermore

$$\begin{aligned}\sigma(\phi+\psi)(x,y) &= \sigma((\phi+\psi)(\sigma^{-1}(x),\sigma^{-1}(y))) = \\ &= \sigma(\phi(\sigma^{-1}(x),\sigma^{-1}(y))+\psi(\sigma^{-1}(x),\sigma^{-1}(y))) \overset{*}{=} \\ &\overset{*}{=} \sigma(\phi(\sigma^{-1}(x),\sigma^{-1}(y)))+\sigma(\psi(\sigma^{-1}(x),\sigma^{-1}(y))) = \\ &= \sigma\phi(x,y)+\sigma\psi(x,y)\end{aligned}$$

where the equality (*) holds because the group law of the curve is a rational function with rational coefficients. The last equality implies that $\sigma(\phi+\psi) = \sigma\phi+\sigma\psi$, then σ is a homomorphism. Finally, σ is injective because if $\sigma\phi = \sigma\psi$ then $\phi = \sigma^{-1}\sigma\phi = \sigma^{-1}\sigma\psi = \psi$. □

Corollary 2.2.3. *Let $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $E \in \mathcal{ELL}(R) \implies \sigma E \in \mathcal{ELL}(R)$*

Proof. $\mathrm{End}(\sigma E) \cong \mathrm{End}(E) \cong R$. □

Remark 2.2.4. If $E \in \mathcal{ELL}(\mathcal{O}_K)$ then σE represents a finite number of curves up to isomorphisms as σ varies in $\mathrm{Aut}(\mathbb{C})$, because $\mathcal{ELL}(\mathcal{O}_K)$ is a finite set.

Theorem 2.2.5. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$, then $[\mathbb{Q}(j(E)):\mathbb{Q}] \le h_K$, where $h_K = |Cl(K)|$ is the class number of K.*

Proof. We know that for every curve $E:\ y^2 = x^3 + ax + b$ we have that $\sigma E:\ y^2 = x^3 + \sigma(a)x + \sigma(b)$, hence

$$j(\sigma E) = 1728\frac{\sigma(a)^3}{4\sigma(a)^3 + 27\sigma(b)^2} = \sigma\left(1728\frac{a^3}{4a^3 + 27b^2}\right) = \sigma(j(E))$$

Thanks to remark 2.2.4 we know that as σ varies in $\mathrm{Aut}(\mathbb{C})$ we obtain a finite number of curves σE up to isomorphism, however j is invariant under isomorphism, then as σ varies in $\mathrm{Aut}(\mathbb{C})$, $j(\sigma E) = \sigma(j(E))$ can take on a finite number of values, in particular at most $h_K = |\mathcal{ELL}(\mathcal{O}_K)|$ values. Let $j_1, ..., j_r$, where $r \leq h_K$, be the admissible values of $j(\sigma E)$ as σ varies in $\mathrm{Aut}(\mathbb{C})$, let's consider the polynomial $p(x) = \prod_{i=1}^{r}(x - j_i)$, then we note that

$$\sigma(p(x)) = \sigma(\prod_{i=1}^{r}(x - j_i)) = \prod_{i=1}^{r}(x - \sigma(j_i)) = \prod_{i=1}^{r}(x - j_i) = p(x)$$

in fact $\sigma(j_i) \in \{j_1, ..., j_r\}$, and $i \neq l \implies \sigma(j_i) \neq \sigma(j_l)$, otherwise

$$\sigma(j_i) = \sigma(j_l) \ \Rightarrow\ j_i = \sigma^{-1}\sigma(j_i) = \sigma^{-1}\sigma(j_l) = j_l$$

which is absurd. Therefore, if $p(x)$ is fixed by every $\sigma \in \mathrm{Aut}(\mathbb{C})$ it means that $p(x) \in \mathbb{Q}[x]$, furthermore $p(j(E)) = 0$, hence $j(E)$ is algebraic. At this point it easy to note that we can estimate the degree of $j(E)$ by taking

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \deg(p(x)) \leq h_K$$

□

Corollary 2.2.6. *If $\mathcal{O}_K$ is a UFD and $E \in \mathcal{ELL}(\mathcal{O}_K)$, then $j(E) \in \mathbb{Q}$.*

CHAPTER 3

Integrity of the j-invariant

In this chapter we introduce the Tate curve and we will use it to prove that the j-invariant of the curves in $\mathcal{ELL}(\mathcal{O}_K)$ is an integer. We will sometimes omit the proof of some following proposition; they can be found in capters I and V of Silverman's book [Sil94].
Before we can start, we need to generalize theorem 1.2.17 in the following way:

Theorem 3.0.1. *Let K be a field of characteristic different from 2 and 3, let $c \in \bar{K}$, then there exists an elliptic curve E defined over $K(c)$ such that $j(E) = c$.*

Proof. If $c = 0$ then it suffices to consider the curve $y^2 = x^3 + 1$.
If $c = 1728$ then it suffices to consider the curve $y^2 = x^3 + x$.
If else $c \neq 0, 1728$, we can define $\gamma = \frac{4}{27}\left(\frac{1728}{c} - 1\right) \in K$ and we have $\gamma \neq 0$. Hence $c = \frac{1728}{1+\frac{27}{4}\gamma}$, in particular we note that $K(c) = K(\gamma)$, then it suffices to find a curve E defined over $K(\gamma)$ such that $j(E) = c$. If we consider the curve $E:\ y^2 = x^3 + \frac{1}{\gamma}x + \frac{1}{\gamma}$ it easy to see that it is defined over $K(\gamma)$, moreover

$$j(E) = 1728\frac{4\frac{1}{\gamma^3}}{4\frac{1}{\gamma^3} + 27\frac{1}{\gamma^2}} = \frac{1728}{1 + \frac{27}{4}\gamma} = c$$

□

In the previous chapter we proved that a complex elliptic curve whose endomorphism ring is isomorphic to a certain ring of integers $\mathcal{O}_K$ which is a UFD, has a rational j-invariant, therefore the last theorem ensures that, up to isomorphism over $\mathbb{C}$, we can assume that this curve is defined by an equation with rational coefficients.

3.1 Expansion in q

Let Λ be a complex lattice, we know that we can assume that Λ is a normalized lattice, up to homothety, then $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ where $\Im(\tau) > 0$. Therefore, we have a function that sends every element of the complex upper half-plane in a lattice. We note that defining the function $q(z) = e^{2\pi iz}$ we can define an isomorphism $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$. This function sends the discrete subgroup $\tau\mathbb{Z} < \mathbb{C}/\mathbb{Z}$ to the discrete subgroup $q^{\mathbb{Z}} < \mathbb{C}^*$. In particular, we have defined an isomorphism $\mathbb{C}/\Lambda \cong \mathbb{C}^*/q^{\mathbb{Z}}$.
We can note that considering Λ as a function $\Lambda(\tau) = \mathbb{Z} \oplus \tau\mathbb{Z}$, the Weierstrass function becomes a two variables function $\wp(z, \tau)$. The idea of considering the function $q = e^{2\ piiz}$ derives from the fact that the Weierstrass function is periodic of period 1 both in z and in tau, therefore we would like to rewrite it in the variables 2 $piiz$ and 2 pii tau in a similar way to what is done for Fourier series expansions.

Lemma 3.1.1. *Let* $q = e^{2\pi i\tau}, u = e^{2\pi iz}, F(u, q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2}$. *Then:*

- *F converges absolutely and uniformly in the compact subspaces of $\mathbb{C} \setminus \mathbb{Z} \oplus \tau\mathbb{Z}$*
- *F is an elliptic function for the lattice $\mathbb{Z} \oplus \tau\mathbb{Z}$, the points $z \in \mathbb{Z} \oplus \tau\mathbb{Z}$ are poles of order 2 and there are no other poles.*
- *The Laurent series of F in $z = 0$ is*

$$F(u, q) = \frac{1}{(2\pi iz)^2} - \left(\frac{1}{12} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2} \right) + (\textit{powers of } z)$$

We omit the proof of this lemma as it only consists in some long calculations. This proof can be found in the lemma [Sil94, chapter 1, lemma 6.1]. This lemma will be useful to prove the following theorem:

Theorem 3.1.2. *If* $q = e^{2\pi i\tau}$ *e* $u = e^{2\pi iz}$ *then:*

- $\frac{1}{(2\pi i)^2}\wp(z, \tau) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} + \frac{1}{12} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}$
- $\frac{1}{(2\pi i)^3}\wp'(z, \tau) = \sum_{n\in\mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3}$

Proof. Let $F(u,q)$ be as in 3.1.1, hence let's consider the function

$$\frac{1}{(2\pi i)^2}\wp(z,\tau) - F(u,q) - \frac{1}{12} + 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2}$$

by the previous lemmathis is an elliptic function holomorphic in $\mathbb{C}\setminus\mathbb{Z}\oplus\tau\mathbb{Z}$. Expanding $\wp(z,\tau)$ and $F(u,q)$ as in lemma 3.1.1 we obtain the function

$$\frac{1}{(2\pi i)^2}\left(\frac{1}{z^2} + \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}\left(\frac{1}{(z-m-n\tau)^2} - \frac{1}{(m+n\tau)^2}\right)\right) - \frac{1}{(2\pi i z)^2} +$$
$$+ \text{(powers of z)} =$$
$$= \frac{1}{(2\pi i)^2}\sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}\left(\frac{1}{(z-m-n\tau)^2} - \frac{1}{(m+n\tau)^2}\right) + \text{(powers of z)}$$

Therefore it is not difficult to notice that this function is holomorphic bi-periodic everywhere, hence limited and then constant. But since it vanishes in 0 we deduce that it is constantly 0, And then we get $wp(z,\ tau)$.
In order to obtain $\wp'(z,\tau)$ we just need to derive with $\frac{d}{dz} = 2\pi i u\frac{d}{du}$ the function $\wp(z,\tau)$. □

Proposition 3.1.3. *If $j(\tau)$ is the j-invariant of the lattice $\mathbb{Z}\oplus\tau\mathbb{Z}$, then*

$$j(\tau) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$$

where $c(n)\in\mathbb{Z}\ \forall n\in\mathbb{N}$.

We omit the proof of this proposition as it is again a long bunch of calculations on the q-expansion of the modular functions. For a reference, one can read [Sil94, chapter 1, prop. 7.4].

Theorem 3.1.4. *Let $u,q\in\mathbb{C}$ such that $|q|<1$, we define*

$$s_k(q) = \sum_{n\geq 1}\frac{n^k q^n}{1-q^n}$$
$$a_4(q) = -5s_3(q) \qquad a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}$$
$$X(u,q) = \sum_{n\in\mathbb{Z}}\frac{q^n u}{(1-q^n)^2} - 2s_1(q)$$
$$Y(u,q) = \sum_{n\in\mathbb{Z}}\frac{(q^n u)^2}{(1-q^n)^3} + s_1(q)$$
$$E_q:\ y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

Then the following hold:

1. *E_q is an elliptic curve and we have a holomorphic isomorphism*

$$\begin{array}{rccl} \phi: & \mathbb{C}^*/q^{\mathbb{Z}} & \longrightarrow & E_q \\ & u & \longmapsto & \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \\ O & \text{if } u \in q^{\mathbb{Z}} \end{cases} \end{array}$$

   where O is the point at infinity

2. *$a_4(q), a_6(q) \in \mathbb{Z}[[q]]$*

3. *$j(E_q) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$, where the coefficients are just as in 3.1.3*

4. *$\forall E/\mathbb{C}\ \exists q \in \mathbb{C}^*$ with $|q| < 1$ such that $E \cong E_q$*

Proof. 1. If $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ and $E_\Lambda:\ y^2 = 4x^3 - g_2x - g_3$, the isomorphism is given by 3.1.2 with the coordinates change

$$\frac{1}{(2\pi i)^2}x = x' + \frac{1}{12}, \qquad \frac{1}{(2\pi i)^3}y = 2y' + x'$$

which gives the equation $y'^2 + x'y' = x'^3 + a_4x' + a_6$ for

$$\begin{aligned} a_4 &= -\frac{1}{4}\cdot\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{48}, \\ a_6 &= -\frac{1}{4}\cdot\frac{1}{(2\pi i)^6}g_3(\tau) - \frac{1}{48}\cdot\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{1728} \end{aligned}$$

2. We can expand denominators $1 - q^n$ in the series s_k and rearrange the series. Then we notice that $a_4(q) \in \mathbb{Z}[[q]]$, while in the case of $a_6(q)$ we note that

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\sum_{n\geq 1}\left(\sum_{d|n}\frac{5d^3 + 7d^5}{12}\right)q^n$$

   and $5d^3 + 7d^5 \equiv 0(12)$ for all $d \in \mathbb{Z}$, indeed $5d^3 + 7d^5 \equiv 2d + d \equiv 0(3)$ and if d is odd $5d^3 + 7d^5 \equiv d + 3d \equiv 0(4)$, if d is even $d^2(5d + 7d^3) \equiv 0(4)$.

3. The formula in proposition 3.1.3 gives the value of j for the functions in theorem 3.1.2, but by the first point of this theorem we have that $X(u,q)$ and $Y(u,q)$ are obtained by them with a linear coordinates change, hence j doesn't change.

4. By corollary 1.2.18 there exists a normalized lattice $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ such that $E \cong E_\Lambda$, then for the point 1 if $q = e^{2\pi i\tau}$ we get that $E \cong E_q$.

□

3.2 The Tate curve

So far, we have only dealt with elliptic curves over $\mathbb{C}$, however it may also be interesting to consider elliptic curves defined over other fields. In chapter 2 we proved that the j-invariant of a CM curve is algebraic, hence the curve can be defined over a number field $\mathbb{Q}(\alpha)$ up to isomorphism (over $\mathbb{C}$). Therefore we can study the properties of this curve over an extension of $\mathbb{Q}(\alpha)$ which is not contained in $\mathbb{C}$, for instance, if $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(\alpha)$, we can consider the $\mathfrak{p}$-adic completion $K = \mathbb{Q}(\alpha)_{\mathfrak{p}}$. From now on we will refer to p-adic fields as completions of number fields with respect to a prime p, or, equivalently, as finite extensions of $\mathbb{Q}_p$. In particular in this section we will deal with elliptic curves defined over p-adic fields.
As a first observation we note that the approach used to describe complex elliptic curves starting from tori fails in the p-adic case, in fact, if in a p-adic field K existed a discrete non-zero subgroup, this would contain an element $x \neq 0$, so adding p^n times x we would obtain that $p^n x$ belongs to this subgroup $\forall n \in \mathbb{N}$. But since $\lim_{n\to\infty} |p^n x| = 0$, it follows that 0 is an accumulation point and therefore the subgroup cannot be discrete.
However, the q-expantion studied in the complex case, allows us, by analogy, to define an elliptic curve also in the p-adic case, indeed K^* admits discrete subgroups of the type $q^{\mathbb{Z}}$, so we can identify the quotients $K^*/q^{\mathbb{Z}}$ with suitable elliptic curves.

Theorem 3.2.1. *Let K be a p-adic field with absolute value $|\cdot|$, let $q \in K^*$ such that $|q| < 1$, then with the same notation of theorem 3.1.4 we have:*

1. *$a_4(q), a_6(q)$ converges in K, moreover the curve $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ (which from now on we will call the Tate curve) has a j-invariant as in the equation 3.1.3.*

2. *The series $X(u,q), Y(u,q)$ converge for all $u \in \bar{K} \setminus q^{\mathbb{Z}}$, furthermore they define an injective homomorphism*

$$\begin{array}{rccl} \phi : & \bar{K}^*/q^{\mathbb{Z}} & \longrightarrow & E_q(\bar{K}) \\ & u & \longmapsto & \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \\ O & \text{if } u \in q^{\mathbb{Z}} \end{cases} \end{array}$$

3. *The function ϕ of the previous point commutates with the action of the Galois group $\mathrm{Gal}\left(\bar{K}/K\right)$, i.e. $\forall \sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ we have*

$$\sigma \circ \phi(u) = \phi \circ \sigma(u) \qquad \forall u \in \bar{K}^*$$

Proof. 1. a_4 and a_6 converge if the series s_k converge. Since $|q| < 1$, we have that $|1 - q^n| = 1$, hence, it is sufficient to show that the series $\sum_{n\geq 1} |n^k q^n| \leq \sum_{n\geq 1} |q^n|$ converges, and this is true. In the same way, also the series $j(q) = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n$ converge and by theorem 3.1.3 we obtain that this is an identity of formal series in $\mathbb{Z}[[q]]$, then it is an identity for all q for which it converges in a field complete with respect to a place, in particular, in our case, it is an identity over K.

2. Similarly to point 1, it's easy to note that X and Y converge $\forall u \in \bar{K} \setminus q^{\mathbb{Z}}$. X and Y are well defined over $\bar{K}^*/q^{\mathbb{Z}}$ because the multiplication of u by a power of q just rearrenges the terms of the summation. Furthermore, $\forall u \in \bar{K}^*/q^{\mathbb{Z}}$ the point $(X(u,q), Y(u,q))$ belongs to the curve $E_q(\bar{K})$, because the theorem 3.1.4 implies that, in the complex case, X and Y verify the equation of the curve, then this is still true a relation of formal series in $\mathbb{Q}(u)[[q]]$, so it is also true as a relation over $\bar{K}$. The property of being a homomorphism is also inherited by the identity of formal series. Finally, in order to prove that it is injective, it is sufficient to notice that the elements in the kernel are those u such that $\phi(u) = O$ is the point at the infinity, that is, all those values for which X and Y do not converge, which are all and only the elements of $q^{\mathbb{Z}}$. Hence, the kernel is trivial in $\bar{K}^*/q^{\mathbb{Z}}$, then ϕ is injective.

3. The automorphisms that fix K don't change the p-adic norm of an element, then it is not difficult to show that the automorphisms commutate with the limit operation of the series, i.e. that, giver a series $\sum_{n\geq 0} x_n$, then $\sigma \sum_{n\geq 0} x_n = \sum_{n\geq 0} \sigma x_n$. Then we get

$$\begin{aligned}\phi \circ \sigma(u) &= (X(\sigma(u), q), Y(\sigma(u), q)) = \\ &= (X(\sigma(u), \sigma(q)), Y(\sigma(u), \sigma(q))) = \\ &= (\sigma X(u, q), \sigma Y(u, q)) = \\ &= \sigma \circ \phi(u)\end{aligned}$$

□

Lemma 3.2.2. *Let K be a p-adic field and let $\alpha \in \bar{K}$ such that $|\alpha| > 1$, then $\exists! q \in \bar{K}^*$ such that $|q| < 1$ and $j(E_q) = \alpha$, furthermore $q \in K(\alpha)$.*

Proof. We know by 3.1.3 that if $c(-1) = 1$, then

$$j(q) = j(E_q) = \frac{\sum_{n\geq 0} c(n-1)q^n}{q}$$

We call

$$f(q) = \frac{1}{j(q)} = \frac{q}{1 + c(0)q + c(1)q^2 + ...} = q - c(0)q^2 + (c(0)^2 - c(1))q^2 + ... \in \mathbb{Z}[[q]]$$

then $\exists g(q) \in \mathbb{Z}[[q]]$ such that $g(f(q)) = q$ as formal series. Clearly we also have $f(g(q)) = q$. Since $g(q) \in \mathbb{Z}[[q]]$ and $|\alpha| > 1$, the series $g(\frac{1}{\alpha})$ converges in $K(\alpha)$. If we label as q the value of such a series, we see that

$$q = g\left(\frac{1}{\alpha}\right) \quad \Longrightarrow \quad \frac{1}{j(q)} = f(q) = f\left(g\left(\frac{1}{\alpha}\right)\right) = \frac{1}{\alpha}$$

and then $j(q) = \alpha$.
We proved that such a q exists, let's now prove that it is unique. If there existed q, q' such that $|q|, |q'| < 1$ and $j(q) = j(q')$ then we would have $f(q) = f(q')$, hence

$$\begin{aligned} 0 &= |f(q) - f(q')| = \\ &= |q - q'| \cdot |1 - c(0)(q + q') + (c(0)^2 - c(1))(q^2 + qq' + q'^2) + ...| = \\ &= |q - q'| \end{aligned}$$

and then $q = q'$. □

We introduced the Tate curve, then we can study how to apply its properties in order to prove that the j-invariant of CM elliptic curves is an integer. Before doing so, let us introduce the following lemma, which in a certain sense refines the result of theorem 1.2.16.

Lemma 3.2.3. *Let E, E' be two elliptic curves defined over the field K such that $E \cong E'$ over $\bar{K}$, then there exists an extension ${}^{K'}\!/_{K}$ such that $5 \neq [K' : K] \leq 6$ and $E \cong E'$ over K'.*

Proof. We can assume that the curves are in Weierstrass form, indeed it is true up to some linear coordinates changes over K, then let

$$E: \ y^2 = x^3 + ax + b \qquad \text{e} \qquad E': \ y^2 = x^3 + cx + d$$

By the theorem 1.2.16 we know that $j(E) = j(E') = j \in K$, then if $j \neq 0, 1728$, by j's formula we notice that $a, b, c, d \neq 0$, hence we have that

$$\frac{1728}{1 + \frac{27}{4}\frac{b^2}{a^3}} = \frac{1728}{1 + \frac{27}{4}\frac{d^2}{c^3}} \implies \frac{b^2}{a^3} = \frac{d^2}{c^3} \implies \left(\frac{a}{c}\right)^3 = \left(\frac{b}{d}\right)^2$$

Let $\gamma = \frac{bc}{ad} \in K$, then by the previous relation it's easy to notice that $\gamma^2 = \frac{a}{c}$ and $\gamma^3 = \frac{b}{d}$. Then, we see that the function

$$\begin{aligned} x &\longmapsto \gamma x \\ y &\longmapsto \sqrt{\tfrac{b}{d}}y \end{aligned}$$

is an isomorphism $E \longrightarrow E'$, where $\sqrt{\frac{b}{d}}$ is a root of $\frac{b}{d}$. In fact,

$$\left(\sqrt{\frac{b}{d}}y\right)^2 = (\gamma x)^3 + a\gamma x + b \implies$$
$$\implies \frac{b}{d}y^2 = \frac{b}{d}x^3 + \frac{a}{c}\gamma c x + \frac{b}{d}d = \frac{b}{d}(x^3 + cx + d) \implies$$
$$\implies y^2 = x^3 + cx + d$$

Therefore, the curves E, E' are isomorphic over a quadratic (or trivial) extension $K\left(\sqrt{\frac{b}{d}}\right)$.
If else $j = 1728$ we note that $b, d = 0$ and $a, c \neq 0$. Hence we consider the function

$$\begin{aligned} x &\longmapsto \sqrt{\tfrac{a}{c}}x \\ y &\longmapsto \sqrt{\tfrac{a}{c}}\sqrt[4]{\tfrac{a}{c}}y \end{aligned}$$

As we did before, we can show that it is an isomorphism between E and E', in addition, it is defined over $K\left(\sqrt[4]{\frac{a}{c}}\right)$, then it is defined over an extension whose degree is a divisor of 4.
Finally, if $j = 0$ then $a, c = 0$ and $b, d \neq 0$, hence the function

$$\begin{aligned} x &\longmapsto \sqrt[3]{\tfrac{b}{d}}x \\ y &\longmapsto \sqrt{\tfrac{b}{d}}y \end{aligned}$$

is an isomorphism between E and E' defined over $K\left(\sqrt[6]{\frac{b}{d}}\right)$, hence defined over an extension whose degree is a divisor of 6. □

Proposition 3.2.4. *Let K be a p-adic field with valuation v, let E/K be an elliptic curve such that $|j(E)| > 1$, let $\ell > 3$ be a prime such that $\ell \nmid v(j(E))$, then there exists $\sigma \in \mathrm{Gal}(\bar{K}/K)$ that acts on the group $E[\ell] \cong {}^{\mathbb{Z}}\!/_{\ell\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\ell\mathbb{Z}}$ as a matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, i.e. there exist $P_1, P_2 \in E[\ell]$ such that*

$$E[\ell] = < P_1, P_2 > \quad e \quad \sigma(P_1) = P_1, \quad \sigma(P_2) = P_1 + P_2$$

Proof. Let's start considering a finite Galois extension ${}^{L}\!/_{K}$ such that $\ell \nmid [L : K]$, then, if w is the valuation of L that extends v, we have that $w(j(E)) = e_{w/v}v(j(E))$, where $e_{w/v}|[L : K]$ is the ramification index, hence it is coprime with ℓ, therefore $\ell \nmid v(j(E)) \iff \ell \nmid w(j(E))$. So L satisfies the hypothesis of the theorem, moreover, if we prove the statement for L, it would hold also for K, because if we find the automorphism σ in the statement we

have $\sigma \in \mathrm{Gal}(\bar{K}/L) \subset \mathrm{Gal}(\bar{K}/K)$.
By lemma 3.2.2 $\exists q \in K$ such that $E \cong E_q$ over $\bar{K}$, hence, in particular, by lemma 3.2.3, the two curves are isomorphic over a finite extension whose degree is always prime to ℓ, because $\ell > 3$. Therefore we just need to prove the statement for E_q, for which the Galois automorphisms commutate with the isomorphism between the curves. Let $\zeta = \zeta_\ell$, then we can assume that $\zeta \in K$, otherwise we can consider the extension $K(\zeta)/K$ whose degree divides $\ell - 1$, which is coprime with ℓ. Let $Q = q^{\frac{1}{\ell}} \in \bar{K}$ be a fixed ℓ-th root of q, since $v(q) = -v(j(E))$, we have that $(\ell, v(q)) = (\ell, v(j(E))) = 1$, then $K(Q)/K$ is totally ramified of degree ℓ, moreover, since it is a Kummer extension, it is cyclic extension of degree ℓ, hence $\exists \sigma \in \mathrm{Gal}(K(Q)/K)$ such that $\sigma(Q) = \zeta Q$. We note that σ is the automorphism we were looking for.
It is easy to notice that $< \zeta, Q > < \frac{\bar{K}^*}{q^{\mathbb{Z}}}$ is a subgroup with ℓ^2 elements, moreover, every element has an order which is a divisor of ℓ, then the homomorphism of theorem 3.2.1 sends $< \zeta, Q >$ into ℓ-torsion points of the curve E_q. However, by theorem 3.2.1, we know that this homomorphism is injective, then by cardinality arguments, it is an isomorphism $\phi : < \zeta, Q > \longrightarrow E[\ell]$. We also know that ϕ commutate with the automorphism σ chosen before, then if $P_1 = \phi(\zeta)$ e $P_2 = \phi(Q)$ we have that

$$\sigma(P_1) = \phi(\sigma(\zeta)) = \phi(\zeta) = P_1$$
$$\sigma(P_2) = \phi(\sigma(Q)) = \phi(\zeta Q) = \phi(\zeta) + \phi(Q) = P_1 + P_2$$

□

Remark 3.2.5. Since ℓ is a prime, P_1, P_2 are a basis of $E[\ell]$ as a $\mathbb{F}_\ell$-space, which is isomorphic to $\mathbb{F}_\ell^2$. Then there exists a representation $\rho_\ell : \mathrm{Gal}(\bar{K}/K) \longmapsto GL_2(\mathbb{F}_\ell)$ which describes how the elements of the Galois group act on the torsion points of the curve, fixed a basis.

Corollary 3.2.6. *Let K be a number field, let E/K be an elliptic curve such that $j(E) \notin \mathcal{O}_K$, then for all primes ℓ but a finite number, there exists $\sigma \in \mathrm{Gal}(\bar{K}/K)$ such that $\rho_\ell(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

Proof. Let p be a prime in $\mathcal{O}_K$ such that $v_p(j(E)) < 0$, let's consider the p-adic completion K_p, since E is defined over K we can assume that it is defined over K_p and $|j(E)| > 1$. If we fix and immersion $\bar{K} \hookrightarrow \bar{K_p}$, this gives an immersion $\mathrm{Gal}(\bar{K_p}/K_p) \subseteq \mathrm{Gal}(\bar{K}/K)$. We know that $\exists \sigma \in \mathrm{Gal}(\bar{K_p}/K_p)$ such that $\rho_\ell(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. However, we have $\sigma \in \mathrm{Gal}(\bar{K}/K)$, in addition, the coordinates of the points in $E[\ell]$ belongs to $\bar{K} \subset \bar{K_p}$, hence the corollary is proved. □

Theorem 3.2.7. *Let K be a number field and let E be an elliptic curver defined over K, then if $j(E) \notin \mathcal{O}_K$ we have that* $\mathrm{End}(E) \cong \mathbb{Z}$.

Proof. Unless you consider a finite extension of K, we know that $\mathrm{End}_{\mathbb{C}}(E) = \mathrm{End}_K(E)$, indeed $\mathrm{End}_{\mathbb{C}}(E)$ is finitely generated over $\mathbb{Z}$, then it's enough to consider the field of definition of its generators, which is a finite extension by lemma 3.2.3. If we manage to prove the theorem for a finite extention of K we have proved it also for K, because the endomorphisms over K form a subset of the endomorphisms over every extension. We also know that $|j(E)| > 1$, then we can choose a prime ℓ big enough satisfying the hypothesis of corollary 3.2.6, in particular, by that corollary, there exists a basis P_1, P_2 of $E[\ell]$ and an automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K)$ such that σ acts as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_\ell)$. Let $\phi \in \mathrm{End}(E)$, taking the restriction of ϕ to $E[\ell]$ is still an endomorphism, then it can be written as a matrix $\phi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_\ell)$, then we have obtained a homomorphism

$$\begin{array}{rccc} \Phi_\ell : & \mathrm{End}(E) & \longrightarrow & M_2(\mathbb{F}_\ell) \\ & \phi & \longmapsto & \phi_\ell \end{array}$$

As the endomorphisms are defined over the field fixed by the Galois group, ϕ commutate with σ, therefore

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

so

$$\begin{cases} a + c = a \\ b + d = a + b \end{cases} \implies c = 0 \wedge a = d$$

hence $\phi_\ell = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$.

Let's now suppose that $\mathbb{Z} \subsetneq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ for $d \in \mathbb{N}$, i.e. that $\mathrm{End}(E)$ is an order in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, then we can assume that ℓ splits in $\mathbb{Q}(\sqrt{-d})$, because in every number field there exists an infinite number of split primes. We can also assume that $\ell \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} : \mathrm{End}(E)]$, because the index is a finite number. Then we can see that the $\mathbb{Z}$-module $\ell\,\mathrm{End}(E)$ is sent to 0 by Φ_ℓ, moreover, if $\phi \in \ker \Phi_\ell$, as an element of $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ is a multiple of ℓ, hence $\ker \Phi_\ell = \ell\,\mathrm{End}(E)$. Therefore, Φ_ℓ is an injective map by taking the quotient by the kernel:

$$\overline{\Phi}_\ell : \frac{\mathrm{End}(E)}{\ell\,\mathrm{End}(E)} \longrightarrow M_2(\mathbb{F}_\ell)$$

In particular $\frac{\mathrm{End}(E)}{\ell\,\mathrm{End}(E)} \cong \mathrm{End}(E) \otimes \frac{\mathbb{Z}}{\ell\mathbb{Z}}$, hence

$$\mathrm{End}(E) \otimes \mathbb{F}_\ell = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell = \frac{\mathbb{Z}[x]}{(x^2+d)} \otimes \mathbb{F}_\ell = \frac{\mathbb{F}_\ell[x]}{(x^2+d)} =$$
$$= \frac{\mathbb{F}_\ell[x]}{(x+\sqrt{d})} \times \frac{\mathbb{F}_\ell[x]}{(x-\sqrt{d})} \cong \mathbb{F}_\ell^2$$

where the first equality holds because $\ell \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} : \mathrm{End}(E)]$, the second because $\ell \neq 2$, and the fourth is a consequence of the chinese remainder theorem by noting that ℓ splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, then x^2+d is reducible.
We notice that

$$|\,\mathrm{End}(E) \otimes \mathbb{F}_\ell| = |\mathbb{F}_\ell^2| = \ell^2 = \left| \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \right\} \right|$$

then by the injectivity of $\overline{\Phi}_\ell$ and by the equality between cardinalities we get that $\overline{\Phi}_\ell$ is surjective onto $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \right\}$, then it is an isomorphism between that set and $\mathrm{End}(E) \otimes \mathbb{F}_\ell$. Then there exists $\phi \in \mathrm{End}(E) \otimes \mathbb{F}_\ell$ such that $\phi_\ell = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, but this is absurd because there are no nilpotent elements in $\mathbb{F}_\ell^2$. □

Corollary 3.2.8. *Let $K = \mathbb{Q}(\sqrt{-d})$ such that $\mathcal{O}_K$ is a UFD, let $E \in \mathcal{ELL}(\mathcal{O}_K)$, then $j(E) \in \mathbb{Z}$.*

Proof. By the corollary 2.2.6 we know that $j(E) \in \mathbb{Q}$, moreover $\mathrm{End}(E) \supsetneq \mathbb{Z}$, then by theorem 3.2.7 $j(E) \in \mathcal{O}_\mathbb{Q} = \mathbb{Z}$. □

CHAPTER 4

Proof of the Gauss conjecture

Proposition 4.0.1. *Let $d \in \mathbb{Z}$ be squarefree such that $d > 2$ and $d \not\equiv 3(4)$, if $K = \mathbb{Q}(\sqrt{-d})$ then $\mathcal{O}_K$ is not a UFD.*

Proof. We have $-d \not\equiv 1(4)$, therefore $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. In order to prove that it is not a UFD we will show that 2 is irreducible but not prime. If there exists $a + b\sqrt{-d}$ such that $a + b\sqrt{-d}|2$, by taking its norm we will obtain $a^2 + b^2 d|4$. However, by hypothesis, $d \geq 5$, then $b = 0$ and $a \in \{\pm 1, \pm 2\}$, that is $a + b\sqrt{-d}$ is invertible or equal to 2 up to multiplication by an invertible element, hence 2 is irreducible.
We notice that if d is even, then $2| - d$ but $2 \nmid \pm\sqrt{-d}$, otherwise if d is odd $2|1 + d$ but $2 \nmid 1 \pm \sqrt{-d}$, then 2 is not a prime. □

Proposition 4.0.2. *Let $d \equiv 3(4)$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ is a UFD, then $\forall p \in \mathbb{Z}$ such that $p < \frac{d}{4}$, p is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.*

Proof. We have $-d \equiv 1(4)$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$. Let's suppose that p is not inert, then

$$\begin{aligned} p &= \left(a + b\frac{1+\sqrt{-d}}{2}\right)\left(a + b\frac{1-\sqrt{-d}}{2}\right) = \\ &= a^2 + ab + b^2\frac{d+1}{4} = \\ &= a^2 + ab + b^2 + b^2\frac{d-3}{4} \;>\; \frac{d-3}{4} \end{aligned}$$

Therefore if $p < \frac{d}{4}$ then it is inert. □

Definition 4.0.3. Let E be a rational elliptic curve, we define the field of definition of the endomorphisms to be the smallest field $K/\mathbb{Q}$ such that $\mathrm{End}_K(E) = \mathrm{End}_{\mathbb{C}}(E)$.

Lemma 4.0.4. *Let E be a rational elliptic curve, let K be its field of definition of the endomorphisms, then $[K : \mathbb{Q}] \leq 2$.*

Proof. We know that if $\mathrm{End}(E) \cong \mathbb{Z}$ then $K = \mathbb{Q}$, so we easily get the thesis, otherwise we know that $\mathrm{End}_{\mathbb{C}}(E) \cong \mathbb{Z}[\omega]$ as rings, where ω is an algebraic integer of degree 2, hence it satisfies an equation $\omega^2 = a\omega + b$ with $a, b \in \mathbb{Z}$. We also know that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{End}_{\mathbb{C}}(E)$ by acting on its coefficients, then there is a homomorphism

$$\Psi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mathrm{End}_{\mathbb{C}}(E)) \cong \mathrm{Aut}(\mathbb{Z}[\omega])$$

Let us consider $\mathrm{Aut}(\mathbb{Z}[\omega])$: if $\phi \in \mathrm{Aut}(\mathbb{Z}[\omega])$ then $\phi(1) = 1$, moreover $\phi(\omega^2 - a\omega - b) = \phi(0) = 0$, hence $\phi(\omega)^2 - \phi(a)\phi(\omega) - \phi(b) = \phi(\omega)^2 - a\phi(\omega) - b = 0$. Therefore, $\phi(\omega)$ can assume only two values, then $\mathrm{Aut}(\mathbb{Z}[\omega]) \cong \mathbb{Z}/2\mathbb{Z}$.
If K is the field of definition of the endomorphisms, $\mathrm{Gal}(\bar{\mathbb{Q}}/K) = \ker \Psi$, in particular $[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) : \mathrm{Gal}(\bar{\mathbb{Q}}/K)] \leq 2$ and this concludes the proof. □

Remark 4.0.5. As we have already remarked, there exists an action

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$$

the we can restrict it to another action

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \longrightarrow GL_2(\mathbb{F}_\ell)$$

and since $[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) : \mathrm{Gal}(\bar{\mathbb{Q}}/K)] = 2$ we obtain that

$$[\rho_\ell \left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right) : \rho_\ell \left(\mathrm{Gal}(\bar{\mathbb{Q}}/K)\right)] \leq 2$$

Given the complex quadratic field $\mathbb{Q}(\sqrt{-d})$, let $2 \neq \ell \in \mathbb{Z}$ be an inert prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell = \frac{\mathbb{Z}[x]}{(x^2 + d)} \otimes \mathbb{F}_\ell = \frac{\mathbb{F}_\ell[x]}{(x^2 + d)} \cong \mathbb{F}_{\ell^2}$$

Therefore, given an elliptic curve $E \in \mathcal{ELL}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ we know that the endomorphisms act on the ℓ-torsion points, in particular $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \otimes \mathbb{F}_\ell \cong \mathbb{F}_{\ell^2}$ faithfully acts on $E[\ell]$. Hence, by cardinality arguments, we get that $E[\ell]$ is a $\mathbb{F}_{\ell^2}$-space of dimension 1, and the endomorphisms act as the multiplication by a scalar. Therefore we deduce that if K is the field of definition of the endomorphisms, then $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ commutates with the endomorphisms, because they are rational function and σ fixes their coefficients, so σ is a linear endomorphism of $E[\ell]$as $\mathbb{F}_{\ell^2}$-space.

Proposition 4.0.6. *Let $E \in \mathcal{ELL}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ be a rational elliptic curve, let $2 \neq \ell \in \mathbb{N}$ be an inert prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, then there exists a basis of $E[\ell]$ such that*

$$\rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right) \subseteq N_{GL_2(\mathbb{F}_\ell)}\left(\left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell)\right\}\right)$$

Proof. Let $0 \neq v \in E[\ell]$, then $v, \sqrt{-d}\cdot v$ is a basis of $E[\ell]$ as $\mathbb{F}_\ell$-space, where $\sqrt{-d}$ is an element of $\mathrm{End}(E) \cong \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Indeed, given $a, b \in \mathbb{F}_\ell$ we have that

$$\begin{aligned} & av + b\sqrt{-d}b = 0 \iff \\ \iff & (a + b\sqrt{-d})v = 0 \iff \\ \iff & a + b\sqrt{-d} = 0 \text{ in } \mathrm{End}(E) \otimes \mathbb{F}_\ell \iff \\ \iff & a, b = 0 \end{aligned}$$

As in theorem 3.2.7, we can represent $\mathrm{End}(E) \otimes \mathbb{F}_\ell$ in $M_2(\mathbb{F}_\ell)$ by considering the restriction of the endomorphisms to the ℓ-torsion points. With this choice of a basis, we get that, given an endomorphism $a + b\sqrt{-d} \in \mathrm{End}(E) \otimes \mathbb{F}_\ell$,

$$\begin{cases} (a + b\sqrt{-d})v = av + b(\sqrt{-d}v) \\ (a + b\sqrt{-d})(\sqrt{-d}v) = -dbv + a(\sqrt{-d}v) \end{cases} \implies (a + b\sqrt{-d}) \mapsto \begin{pmatrix} a & -db \\ b & a \end{pmatrix}$$

Moreover, since ℓ is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, we have the isomorphism $\mathrm{End}(E) \otimes \mathbb{F}_\ell \cong \mathbb{F}_{\ell^2}$. Let's call

$$C := \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell)\right\} = \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in M_2(\mathbb{F}_\ell) \middle| (a, b) \neq (0, 0)\right\}$$

we can notice that $C \cong (\mathrm{End}(E) \otimes \mathbb{F}_\ell)^* \cong \mathbb{F}_{\ell^2}^*$ then it is a cyclic group.
As remarked above, the elements of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ commutate with the endomorphisms, hence

$$H := \rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/K)) \subseteq Z_{GL_2(\mathbb{F}_\ell)}(C) \subseteq N_{GL_2(\mathbb{F}_\ell)}(C)$$

If $\rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) = H$ then the previous inclusion would conclude the proof; so, we just have to consider the case $[\rho_\ell(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) : H] = 2$. We begin by showing that

$$N := N_{GL_2(\mathbb{F}_\ell)}\left(\left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix}\right\}\right) = \left\{\begin{pmatrix} a & -db \\ b & a \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} a & db \\ b & -a \end{pmatrix}\right\}$$

Let $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{F}_\ell)$ such that $\forall \begin{pmatrix} a & -db \\ b & a \end{pmatrix} \in C \quad \exists \begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix} \in C$ satisfying the equation

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & -db \\ b & a \end{pmatrix} = \begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{4.1}$$

since the trace is invariant by conjugation, thanks to the equation 4.1 we get that

$$Tr \begin{pmatrix} a & -db \\ b & a \end{pmatrix} = Tr \begin{pmatrix} a' & -db' \\ b' & a' \end{pmatrix} \implies 2a = 2a' \implies a = a'$$

The same equation gives, by taking the determinants,

$$a^2 + db^2 = a + db'^2 \implies b = \pm b'$$

If we choose matrices such that $b \neq 0$, with some calculations we obtain that:

$$\begin{cases} a\alpha + b\beta = a\alpha \mp db\gamma \\ -db\alpha + a\beta = a\beta \mp db\delta \\ a\gamma + b\delta = \pm b\alpha + a\gamma \\ -db\gamma + a\delta = \pm b\beta + a\delta \end{cases} \implies \begin{cases} \alpha = \pm\delta \\ \beta = \mp d\gamma \end{cases}$$

Hence we obtained that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & -d\gamma \\ \gamma & \alpha \end{pmatrix} \quad \vee \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & d\gamma \\ \gamma & -\delta \end{pmatrix}$$

then we get the desired equality.
It is not difficult to notice that if in the equation 4.1 the two matrices in C are the same, i.e. if $(a, b) = (a', b')$, with the same calculations we get that $\alpha = \delta$ and $\beta = -d\gamma$. Then $Z_{GL_2(\mathbb{F}_\ell)}(C) \subseteq C$, moreover we know that C is a cyclic group, hence $Z_{GL_2(\mathbb{F}_\ell)}(C) = C$.
Therefore $H \subseteq C$. Let $H' = \rho_\ell\left(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\right)$, we know that $[H' : H] = 2$, in particular $H \lhd H'$, then $H' \subseteq N_{GL_2(\mathbb{F}_\ell)}(H)$. If we manage to prove that $N_{GL_2(\mathbb{F}_\ell)}(H) \subseteq N$ then the thesis follows.
Let's assume that $H < C$ contains an element different from a multiple of the identity, then it is a matrix of the form $\begin{pmatrix} a & -db \\ b & a \end{pmatrix}$, with $b \neq 0$. If $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in N_{GL_2(\mathbb{F}_\ell)}(H)$ then it should verify the equation 4.1 with such a, b and with some a', b'; however, since $b \neq 0$, in the same way we obtain that $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in N$, in

particular $N_{GL_2(\mathbb{F}_\ell)}(H) \subseteq N$.
If else every element in H is a multiple of the identity, then H consists of multiples of the identity for every basis of $E[\ell]$ we can choose, because the conjugation in $GL_2(\mathbb{F}_\ell)$ fixes the elements of H. Let $h \in H' \setminus H$, we know that the quotient H'/H is cyclic and has order 2, then $H' =< h, H >$; hence we just need to find a basis such that $h \in N$, so that $H' =< h, H > < N$. Since $[H' : H] = 2$, h is such that $h^2 = \lambda I$ for some $\lambda \in \mathbb{F}_\ell^*$, then its minimal polynomial divides $x^2 - \lambda$, in particular its eigenvalues belong to the set $\{\pm\sqrt{\lambda}\}$. Let's treat this two cases separately:

- λ **is a square in** $\mathbb{F}_\ell$**:** then there are two sub-cases: either h is similar to $\pm\sqrt{\lambda}I$ or it is similar to $\begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & -\sqrt{\lambda} \end{pmatrix}$, in fact,it cannot be a Jordan block because its minimal polynomial has roots with multiplicity 1. Such matrices belong to N, hence h, considered in the basis for which it is diagonal, belongs to N, then the thesis follows.

- λ **is not a square in** $\mathbb{F}_\ell$**:** since h is not a multiple of the identity, there exists $v \in E[\ell]$ such that v, hv are a basis of $E[\ell]$. With such a basis $h(v) = (hv)$ and $h(hv) = \lambda v$, then h is the matrix $\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$. Since ℓ is inert in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ we know that $-d$ is not a square modulo ℓ, then $\exists \mu \in \mathbb{F}_\ell$ such that $\mu^2 = \frac{\lambda}{-d}$. Then by conjugating the matrix $\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}$ by the matrix $\begin{pmatrix} \mu^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ we obtain

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \mu^{-1}\lambda \\ \mu & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\mu d \\ \mu & 0 \end{pmatrix} \in C$$

  Hence we founnd a basis such that $h \in N$, then the thesis follows.

□

At this point, we will try to put together the results obtained to find the rings of the integers of imaginary quadratic fields with unique factorization. When Gauss worked out his conjecture he calculated the class number of all the first imaginary quadratic fields, finding that for $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ is a UFD. In particular he verified that for $d \leq 163$ they are the only fields with class number equal to 1. In order to prove that they are the only fields with this property we can therefore assume that $d > 163$. Let $K = \mathbb{Q}(\sqrt{-d})$ as usual, suppose that $\mathcal{O}_K$ is a UFD, then by proposition 4.0.1 we know that $d \equiv 3(4)$, then by proposition 4.0.2 all primes

$p < \frac{d}{4}$ are inert in K, in particular, all primes smaller than 41 are inert in K. Let us now introduce the following theorem which will be necessary to prove the conjecture.

Theorem 4.0.7. *Let $\ell \in \mathbb{N}$ be a prime number, then there exists a curve $Y_{ns}^{+}(\ell)$ defined over $\mathbb{Q}$ such that there exists a correspondence*

$$Y_{ns}^{+}(\ell)(\mathbb{Q}) \longleftrightarrow \left\{ j(E) \middle| \ E/\mathbb{Q} \ , \ \rho_{E,\ell}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \subseteq N_{GL_2(\mathbb{F}_\ell)}(C) \right\}$$

where the inclusion holds in a suitable basis of $E[\ell]$ and where, fixed $\epsilon \in \mathbb{F}_\ell^* \setminus \mathbb{F}_\ell^{*2}$,

$$C = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \in GL_2(\mathbb{F}_\ell) \right\}$$

We will omit the proof of this theorem, which is long and difficult. The reader can see the book of Deligne and Rapoport [DR73] or Siksek's notes [Sik] for a reference. We will try to explain in broad terms how the curve $Y_{ns}^{+}(\ell)$ can be found. The group so far labeled as C is called non-split Cartan subgroup; it is generally written as $C_{ns}(\ell)$, while its normalizer is written as $C_{ns}^{+}(\ell)$. Let $X(\ell)$ be the compact modular curve that classifies the isomorphism classes of elliptic curves with complete level-ℓ structure. We can define the curves

$$X_{ns}(\ell) := X(\ell)/C_{ns}(\ell) \qquad \text{e} \qquad X_{ns}^{+}(\ell) := X(\ell)/C_{ns}^{+}(\ell)$$

which are the compact modular curves of the groups $C_{ns}(\ell)$ e a $C_{ns}^{+}(\ell)$ respectively. We call $Y_{ns}(\ell)$ and $Y_{ns}^{+}(\ell)$ the respective non-compact modular curves. For small values of ℓ, in particular for $\ell \leq 7$ (the one we will need to complete the proof of the conjecture), the curve $X_{ns}^{+}(\ell)$ is rational, i.e. isomorphic to $\mathbb{P}^1\mathbb{Q}$. By fixing an isomorphism $\mathbb{P}^1\mathbb{Q} \longrightarrow X_{ns}^{+}(\ell)$ we can parametrize all the point of $Y_{ns}^{+}(\ell)(\mathbb{Q})$ with $u \in \mathbb{Q}$ but a finite set of points, corresponding to the cusps of $X_{ns}^{+}(\ell)$.
By definition, there exists a morphism j such that

$$j : X_{ns}^{+}(\ell) \longrightarrow \frac{X(\ell)}{GL_2(\mathbb{F}_\ell)} \cong X(1) \cong \mathbb{P}^1$$

and given $P \in X_{ns}^{+}(\ell)(\mathbb{Q})$, by theorem 4.0.7 it represents an elliptic curve E, moreover $j(P) = j(E)$.
We know that all primes $\ell < 41$ are inert in K, then by proposition 4.0.6, given a curve $E \in \mathcal{ELL}(\mathcal{O}_K)$, the image of ρ_ℓ is contained in $C_{ns}^{+}(\ell)$, hence, thank to theorem 4.0.7, E corresponds to a point P_3 of $X_{ns}^{+}(3)(\mathbb{Q})$ and to a point P_7 of $X_{ns}^{+}(7)(\mathbb{Q})$. These points correspond to some rational numbers u_3

and u_7. Since we can explicit the equations of $X_{ns}^+(3)(\mathbb{Q})$ and $X_{ns}^+(7)(\mathbb{Q})$, we obtain

$$j(E) = j_3(u_3) = u_3^3 \tag{4.2}$$

$$j(E) = j_7(u_7) = 64\frac{(u_7(u_7^2+7)(u_7^2-7u_7+14)(5u_7^2-14u_7-7))^3}{(u_7^3-7u_7^2+7u_7+7)^7} \tag{4.3}$$

These equations can be found in Baran's article [Bar10]. From now on we will write $u = u_7$.
Since $\mathcal{O}_K$ is a UFD, by corollary 3.2.8 we know that $j(E) \in \mathbb{Z}$. In particular, by equation 4.3, we obtain that

$$j(E) = j_7(u) = 64\frac{(u(u^2+7)(u^2-7u+14)(5u^2-14u-7))^3}{(u^3-7u^2+7u+7)^7} \in \mathbb{Z}$$

If we solve this equation we can restrict the set of possible elliptic curves whose ring of endomorphisms has unique factorization. First of all, since the equation is defined over $\mathbb{P}^1\mathbb{Q}$, by calculating j_7 at the point at infinity we obtain $j_7(\infty) = 2^6 \cdot 5^3 = 8000$, then ∞ is a solution of the equation and therefore leads to an admissible value of j. Now we can restrict the equation to $\mathbb{Q}$. Let's call

$$f(u) = u(u^2+7)(u^2-7u+14)(5u^2-14u-7) \quad \text{e} \quad g(u) = u^3-7u^2+7u+7$$

then, since $f(u), g(u) \in \mathbb{Z}[u]$, there exist two polynomials $a(u), b(u) \in \mathbb{Z}[u]$ such that

$$f(u)a(u) + g(u)b(u) = r$$

where $r \in \mathbb{Z}$ is the resultant of f and g. It's easy to notice that $\deg(af) = \deg(bg) = n$, then, if we write $u = \frac{X}{Y}$ with $X, Y \in \mathbb{Z}$ coprimes, we can homogenize the polynomials f and g in the following way

$$F(X,Y) = f\left(\frac{X}{Y}\right)\cdot Y^7 \qquad \text{e} \qquad G(X,Y) = g\left(\frac{X}{Y}\right)\cdot Y^3$$

and replacing it in the equation we obtain

$$F(X,Y)A(X,Y) + G(X,Y)B(X,Y) = rY^n$$

Therefore, fixed two coprime integers X and Y, one can note that

$$(G(X,Y), F(X,Y))|rY^n$$

moreover $G(X,Y) = X^3 - 7X^2Y + 7XY^2 + 7Y^3$, then by euclidean division we obtain that $(G(X,Y), Y) = (X^3, Y) = 1$, in particular $(G(X,Y), Y^n) = 1$, and so

$$(G(X,Y), F(X,Y))|r$$

We know that

$$64\frac{f(X/Y)^3}{g(X/Y)^7} = 64\frac{F(X,Y)^3}{G(X,Y)^7} \in \mathbb{Z}$$

therefore, if $p \in \mathbb{Z}$ is prime such that $p|G(X,Y)$, necessarily $p|2F(X,Y)$, then $p|2r$.
One can compute the resultant obtaining $r = -26985857024 = -2^{15} \cdot 7^7$, then $p = 2 \vee p = 7$. We notice that $7^2 \nmid G(X,Y)$, indeed

$$G(X,Y) \equiv 0(7) \iff X^3 - 7X^2Y + 7XY^2 + 7Y^3 \equiv 0(7) \iff X = 7Z$$

and then we obtain

$$G(7Z,Y) = 7(7^2Z^2 - 7^2Z^2Y + 7ZY^2 + Y^3) \equiv 7(49)$$

since $7 \nmid Y$, because $(X,Y) = 1$.
Let $k = v_2(G(X,Y))$, let's suppose that $k > 15$, hence, since j is an integer,

$$v_2(64F(X,Y)^3) = 6 + 3v_2(F(X,Y)) \geq 7k$$

However $(F(X,Y), G(X,Y))|2^{15} \cdot 7^7$, then $v_2(F(X,Y)) \leq 15$, because $k > 15$. By combining the inequalities we get

$$7k \leq 6 + 3v_2(F(X,Y)) \leq 6 + 3 \cdot 15 = 51$$

which never holds, because $k > 15$. This implies that $v_2(G(X,Y)) \leq 15$. In particular we know that

$$X^3 - 7X^2Y + 7XY^2 + 7Y^3 = 2^a \cdot 7^b \qquad \text{for } 0 \leq a \leq 15\ ,\ 0 \leq b \leq 1$$

However, by the equation 4.2 we know that j mus be a cube, but this is true if and only if $G(X,Y)$ is a cube; hence $a \equiv 0(3)$ and $b \equiv 0(3)$. Therefore, we get 6 equations:

$$X^3 - 7X^2Y + 7XY^2 + 7Y^3 = 2^{3a} \qquad \text{con } 0 \leq a \leq 5$$

These are Thue equations, then they have a finite number of solutions; there exist a way of bound and then compute these solutions. By solving the equations with X and Y being coprimes with $Y \neq 0$ one can find the solutions

$$(2,1),\ (11,2),\ (-19,-9),\ (-5,-1),\ (-3,-1),\ (-3,5),\ (1,-1),\ (1,1)$$

These correspond to the following j-invariants:

Solution	j	j factorization
$(-3,5)$	-262537412640768000	$-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3$
$(2,1)$	-147197952000	$-2^{15}\cdot 3^3\cdot 5^3\cdot 11^3$
$(-5,-1)$	-884736000	$-2^{18}\cdot 3^3\cdot 5^3$
$(1,1)$	-32768	-2^{15}
$(-3,-1)$	1728	$2^6\cdot 3^3$
$(1,-1)$	287496	$2^3\cdot 3^3\cdot 11^3$
$(11,2)$	$6673554058125250 5802048$	$2^6\cdot 11^3\cdot 23^3\cdot 149^3\cdot 269^3$
$(-19,-9)$	$6838755720062350457411072$	$2^9\cdot 17^6\cdot 19^3\cdot 29^3\cdot 149^3$

Each j uniquely identifies a class of isomorphisms of elliptic curves and their endomorphism rings are the possible solutions to our conjecture. Indeed, if $K=\mathbb{Q}(\sqrt{-d})$, for $d>163$, and $\mathcal{O}_K$ is a UFD, then the curve $E\cong {}^{\mathbb{C}}\!/_{\mathcal{O}_K}$ is such that $j(E)$ belongs to the list above. Then we only need to check whether such j, including the value obtained at the point at infinity, produce non-CM elliptic curves or whether the quadratic fields in which their endomorphism rings are immersed have class number 1 or not. Such listed j could also return values of d less than or equal to 163, in which case we can ignore them, as they have already been verified previously.
The next table lists the values of d for which the curves associated with j, up to isomorphism, have as a ring of endomorphisms an order in $\mathbb{Q}(\sqrt{-d})$:

j	j factorization	d
-262537412640768000	$-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3$	163
-147197952000	$-2^{15}\cdot 3^3\cdot 5^3\cdot 11^3$	67
-884736000	$-2^{18}\cdot 3^3\cdot 5^3$	43
-32768	-2^{15}	11
1728	$2^6\cdot 3^3$	1
8000	$2^6\cdot 5^3$	2
287496	$2^3\cdot 3^3\cdot 11^3$	1
$6673554058125250 5802048$	$2^6\cdot 11^3\cdot 23^3\cdot 149^3\cdot 269^3$	non CM
$6838755720062350457411072$	$2^9\cdot 17^6\cdot 19^3\cdot 29^3\cdot 149^3$	non CM

The study of the modular curve $X_{ns}^{+}(7)$ and its integer points to solve the class 1 number problem were addressed by Kenku [Ken85]. At the end of his article he gives a table of values of j which includes those given above. Such values are also listed in Baran's article [Bar10, table 5.4], where all and only the values we have just obtained are shown.

Note that the solutions of the equation led us to obtain some values of d that we had already excluded, since Gauss already verified them. This is because the only hypothesis deriving from the assumption that $d > 163$ consists in the fact that the first $\ell < 41$ are inert in $Q(\sqrt{-d})$, in our specific case, that 3 and 7 are inert in $Q(\sqrt{-d})$. It is therefore logical that the values $d = 43, 67, 163$ appear in our table, since in these cases $3, 7 < \frac{d}{4}$, so by the proposition **??** they are inert. Moreover, it is known that primes 3 modulo 4 are inert in $\mathbb{Q}(i)$, so the value $d = 1$ was also logical to appear. For $d = 11$ we know that $-11 \equiv 3(7)$ is not a square, so $x^2 + 11$ is irreducible in $\mathbb{F}_7$, so 7 is inert in $\mathbb{Q}(\sqrt{-11})$; anyway $11 \equiv 1(3)$ is a square, i.e. 3 is not inert. For $\ell = 3$, however, the normalizer of a split Cartan subgroup is contained in the normalizer of a non-split Cartan subgroup, which justifies the fact that 11 appears in our table. A result in this respect can be found in Serre's book [Ser89, appendix A, A.6]. An analogous discourse is valid for the case $d = 2$. The values found by Gauss which did not appear are $d = 3, 7, 19$, in fact 3 and 7 are respectively ramified in $\mathbb{Q}(\sqrt{-3})$ and in $\mathbb{Q}(\sqrt{-7})$, while $-19 \equiv 2(7)$, so 7 is not inert in $\mathbb{Q}(\sqrt{-19})$.
This completes the proof of the conjecture.

Bibliography

[Bak67] Alan Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[Bar10] Burcu Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. 1973. Lecture Notes in Math., Vol. 349.

[Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Hee52] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[Ken85] Monsuru A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32(1):45–48, 1985.

[Ser89] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[Sik] Samir Siksek. Explicit arithmetic of modular curves. `https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf`.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sta67] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.